AF
2132

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	§	Attorney Docket No. 32849.16 (NR-2)
Robert Daniel Maher III	§	
	§	Customer No. 27683
Serial No. 09/598,631	§	
	§	Group Art Unit: 2132
Filed: June 21, 2000	§	
	§	Examiner: Lemma, Samson B.
For: METHOD AND APPARATUS FOR	§	
PREVENTING DENIAL OF	§	
SERVICE ATTACKS	§	

TRANSMITTAL

Mail Stop APPEAL BRIEFS-PATENT
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Enclosed are the following regarding the above-identified patent application:

1.   Brief on Appeal w/Appendix (in triplicate);
2.   Check in the amount of $500.00; and
3.   Return Post Card.

Also, the Commissioner is hereby authorized to charge any deficiency fees or credit any overpayments associated with this communication to Deposit Account No. 08-1394.

Respectfully submitted,

Steven T. McDonald
Registration No. 45,999

Date: August 10, 2005

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 972-739-8631
Facsimile: 214-200-0853
File: 32849.16 (NR-2)

R113090

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of:	§	Attorney Docket No. 32849.16 (NR-2)
Robert Daniel Maher III	§	
	§	Customer No. 27683
Serial No. 09/598,631	§	
	§	Group Art Unit: 2132
Filed: June 21, 2000	§	
	§	Examiner: Lemma, Samson B.
For: METHOD AND APPARATUS FOR	§	
PREVENTING DENIAL OF	§	
SERVICE ATTACKS	§	

08/12/2005 SHASSEN1 00000024 09598631

01 FC:1402 .   500.00 OP

08/12/2005 SHASSEN1 00000003 09598631

01 FC:1401   500.00 OP

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This Brief is submitted in connection with an appeal from the final rejection of the Examiner, dated March 10, 2005, finally rejecting claims 1-16, all of the pending claims in this application.

REAL PARTY IN INTEREST

The real party in interest is Netrake Corporation, a United States company having a principal office and place of business at 3000 Technology Drive, Suite 100, Plano, TX 75074.

RELATED APPEALS AND INTERFERENCES

There are no related appeals and no related interferences regarding the above-identified patent application.

STATUS OF CLAIMS

Claims 1-16 are pending, stand finally rejected, and are on appeal here. Claims 1-16 are set forth in Appendix A attached hereto.

STATUS OF AMENDMENTS AFTER FINAL REJECTION

No amendments were made after the Final Office Action was filed March 10, 2005.

SUMMARY OF THE INVENTION

The present invention, as set forth in independent claim 1, relates to a method for preventing denial of service attacks over a data network that includes a plurality of traffic flows each formed by a plurality of data packets. Contents of the data packets are scanned (Page 3, Line 20; Page 9, Lines 9-12; and Page 10, Lines 15-19), and the data packets are verified to conform to a set of predetermined requirements (Page 3, Lines 20-25; and Page 17, Lines 5-7). A check if a data packet is associated with a validated traffic flow is made (Page 3, Lines 26-27; Page 11, Lines 19-21; and Page 17, Lines 11-16). The data packet is placed in a higher priority quality of service if the data packet is associated with a validated traffic flow and is placed in a low priority quality of service if it is not associated with a validated traffic flow (Page 3, Lines 27-33; Page 11, Lines 21-24; and Page 17, Lines 21-29).

Another embodiment, as set forth in claim 7, relates to a method for preventing denial of service attacks on a data network which includes a plurality of traffic flows each formed by multiple data packets having header and payload information. A network device comprises a traffic flow scanning engine and a quality of service processor having a low priority queue and higher priority queues (Page 4, Lines 2-3). The header information is scanned using the traffic flow scanning engine (Page 4, Line 3-4). The data packets are reordered and reassembled using the traffic flow scanning engine (Page 4, Lines 7-8). Data packets that do not reorder or reassemble correctly are flagged to be dropped (Page 4, Lines 9-10). The payload contents are

scanned using the traffic flow scanning engine (Page 4, Lines 3-4). A determination is made whether the data packets conform to a set of predetermined requirements (Page 4, Lines 9-11). The data packets that do not conform are flagged to be dropped (Page 4, Lines 9-11). A check if the data packets are associated with a validated traffic flow is made. Data packets are assigned to a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if the data packet is not associated with a validated traffic flow (Page 3, Lines 27-33; Page 4, Lines 16-19; Page 11, Lines 21-24; and Page 17, Lines 21-29).

Another embodiment, as set forth in claim 12, relates to a network device for preventing denial of service attacks on a data network which includes a plurality of traffic flows each formed by multiple data packets having contents including header information and payload information. The network device comprises a traffic flow scanning engine operable to scan the header and payload information of the data packets (Page 4, Lines 3-4), associate each data packet with a particular traffic flow, and determine whether each traffic flow is a validated traffic flow or a non-validated traffic flow (Page 4, Lines 14-19). The traffic flow scanning engine is further operable to reorder and reassemble the data packets and to verify that the data packet conforms to predetermined requirements such that the traffic flow scanning engine produces a conclusion associated with each data packet (Page 4, Lines 9-13). The network device further comprises a quality of service processor connected to the traffic flow scanning engine that is operable to place the data packets into a quality of service queue from a plurality of quality of service queues based on the conclusion from the traffic flow scanning engine. Data packets from non-validated traffic flows are assigned to a low priority queue and data packets from validated traffic flow are assigned to a higher priority queue based on its contents (Page 3, Lines 27-33; Page 4, Lines 16-19; Page 11, Lines 21-24; Page 17, Lines 21-29).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I.   Claims 1-16 stand rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 6,598,034 to Kloth ("Kloth") in view of U.S. Patent No. 6,636,512 to Lorrain et al. ("Lorrain").

ARGUMENT

ISSUE 1

The first issue for the Board's consideration is whether claims 1-16 are unpatentable under 35 U.S.C. §103(a) over Kloth in view of Lorrain. This issue will be discussed with reference to the above identified claim groups.

As detailed below, the Applicant believes that the Examiner has improperly applied the combination of references to the claims. More specifically, it is Applicant's belief that the Examiner cannot factually support a prima facie case of obviousness with respect to the rejected claims because the references, even when combined, fail to teach or suggest the claimed subject matter.

Claims 1, 2, 3, 6, 12, 13, and 15

Applicants traverse the rejection of these claims on the grounds that the references are defective in establishing a prima facie case of obviousness. It is well settled that, in order to reject a patent application for obviousness, the prior art reference must teach or suggest all of the claimed limitations. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Moreover, all words in a claim must be considered in judging the patentability of that claim against the prior art. In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Applicants respectfully submit that even if combined, Kloth and Lorrain clearly do not teach or suggest the limitations of claims 1, 7, and 12.

With respect to the improper application of Kloth and Lorrain, the Applicant submits that neither Kloth and Lorrain, separately or in combination, teach or suggest all of the elements of claim 1 as required by MPEP § 2143. Applicants traverse the rejection of this claim on the grounds that the references are defective in establishing a prima facie case of obviousness.

Claim 1 recites:

> A method for preventing denial of service attacks over a data network including a plurality of traffic flows each formed by a plurality of data packets, the method comprising:
> scanning the contents of the data packets;
> verifying that the data packets conform to a set of predetermined requirements;
> checking if the data packet is associated with a validated traffic flow; and

placing the data packet in a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if it is not associated with a validated traffic flow.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) <u>must teach or suggest all the claim limitations</u>.

The MPEP § 2142 provides:

> ... The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness...

Additionally, MPEP states the following:

MPEP 2111 Claim Interpretation; Broadest Reasonable Interpretation

CLAIMS MUST BE GIVEN THEIR BROADEST REASONABLE INTERPRETATION

During patent examination, the pending claims must be "given the broadest reasonable interpretation consistent with the specification...The broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach..." (in part; emphasis added)

MPEP 2111.01 Plain Meaning (in part):

"PLAIN MEANING" REFERS TO THE MEANING GIVEN TO THE TERM BY THOSE OF ORDINARY SKILL IN THE ART

When not defined by applicant in the specification, the words of a claim must be given their plain meaning. In other words, they must be read as they would be interpreted by those of ordinary skill in the art.

It is submitted that, in the present case, the Examiner has not factually supported a prima facie case of obviousness.

The Final Office Action alleges that Lorrain describes "placing the data packet in a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if it is not associated with a validated traffic flow." Applicants respectfully disagree. The Examiner alleges that the description provided by Lorrain of reserving bandwidth for a higher priority quality of service if the data packet is associated with *Real Time traffic* and serving a packet that is associated with non Real Time traffic with a lower quality of service is sufficient to disclose the subject claim limitation of "placing the data packet in a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if it is not associated with a validated traffic flow." That is, the Examiner has interpreted "Real Time" traffic as validated traffic, and has interpreted "non Real Time" traffic as "non validated traffic." (See Office Action dated 3/10/2005, Page 3).

Applicants submit that the Examiner's interpretation of "validated traffic," as taught by the subject application, as "Real Time traffic," as described by Lorrain, is outside the broadest reasonable interpretation of "validated traffic," and that the Examiner's interpretation of the claim term *validated* is contrary to the plain meaning of the term *validated*. Similarly, Applicants submit that the Examiner's interpretation of traffic that is not validated (or "non-validated") as described in the subject application as "non Real Time traffic," as described by Lorrain, is outside the broadest reasonable interpretation of "non validated" and is contrary to the plain meaning of the term.

As is well known, "real time" is descriptive of traffic that is time or latency sensitive, and non real time traffic is not time or latency sensitive. Validated traffic, as referred to in the subject application, refers to traffic that originates from a valid user or source, and non validated traffic is traffic that originates from a source that has not been validated.

With regard to the term "Real Time traffic," as disclosed by Lorrain, Applicants note the following passage of Lorrain:

> In practice, it is common to reserve bandwidth for high priority packets, (e.g. so-called Real Time (RT) traffic) derived from committed QoS traffic, which are transmitted in preference to lower priority packets derived from discardable traffic (e.g. Non Real Time (NRT) traffic or more particularly Non Reserved (NR) traffic).

Lorrain, Column 2, Lines 20-25

As can be seen, Lorrain makes no description or suggestion of a correlation between real time traffic and validated traffic. Lorrain uses the term *Real Time* is generally consistent with the conventional meaning of the term, and only refers to "high priority" packets as "so called Real Time traffic" and lower priority packets as "Non Real Time" traffic. Lorrain neither describes, suggests or otherwise alludes to validated traffic or non validated traffic and in no manner makes any correlation between *validated and real time* or *non-validated and non real time.*

With regard to the usage of validated and non validated traffic in the subject application, Applicants note the following passages of the subject application:

> Network apparatus 100 can act to quality traffic flows by scanning the contents of the packets and *verifying that the contents contain valid network traffic* between known sources and destinations. Traffic flows *that have not been verified because they are from unknown sources or because they are new unclassified flows* can be *assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic.*

Subject Application, Page 11, Lines 18-24 (*emphasis added*).

Thus, the subject application makes clear that the characterization of traffic as validated and non validated is made in a conventional sense of the term, and Applicants have made no description or suggestion that validated traffic is some manner relates to real time or latency characteristics of the traffic. Similarly, Applicants made no description or suggest that non validated, or non verified, traffic is some manner relates to non real time or latency characteristics of the traffic. Rather, Applicants refer to validated traffic as network traffic from known sources and destinations (e.g., traffic that is not spoofed), and traffic that is not yet classified as valid (i.e., non validated traffic) as traffic that has not been verified because the source is unknown, the flow is new and thus unclassified, or the like.

Thus, it is clear that the Examiner's interpretation of "validated traffic" as "Real Time traffic" is not consistent *with the subject specification* as the specification has made no description or suggestion that validated/non validated traffic has any relation to real time/non real time or other latency characteristics of the traffic. For at least this reason, the interpretation of validated traffic as Real Time traffic and non-validated traffic as non Real Time traffic is in error and is outside the broadest reasonable interpretation of the claim language afforded by the subject application. Accordingly, the interpretation or validated traffic as disclosed by the Real

time traffic described by Lorrain is inconsistent with MPEP 2111. For at least this reason, Lorrain fails to describe or suggest "placing the data packet in a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if it is not associated with a validated traffic flow" as described in the subject application and clearly recited in claim 1.

Moreover, an interpretation of the claim language according to the plain meaning of the claim terms fails to render claim 1 obvious. For example, the following common definitions of *valid* and *real time* are as follows:

> **valid:**
> 1 : having legal efficacy or force; *especially* : executed with the proper legal authority and formalities <a *valid* contract>
> 2 a : well-grounded or justifiable : <u>being at once relevant and meaningful</u> <a *valid* theory> b : <u>logically correct</u> <a *valid* argument> <*valid* inference>
> 3 : appropriate to the end in view : **EFFECTIVE** <every craft has its own *valid* methods>
> **real time:**
> the actual time during which something takes place <the computer may partly analyze the data in *real time* (as it comes in)

Merriam Webster online (<u>emphasis added</u>).

> **valid**
> adjective
> 1 based on truth or reason; able to be accepted:
> **real-time** adjective
> describes computing systems that are able to deal with and use new information immediately and therefore influence or direct the actions of the objects supplying that information

Cambridge Dictionaries Online

Thus, as dictionary definitions of the subject terms indicate, interpretation of validated traffic as real time traffic is inconsistent with the plain meaning given to the terms because the terms valid and real time are wholly unrelated. For at least this reason, Lorrain fails to describe or suggest "placing the data packet in a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if it is not associated with a validated traffic flow" as described in the subject application and clearly recited in claim 1.

Moreover, the subject application clearly distinguishes between placing a data packet in a higher priority quality of service <u>if the data packet is associated with a validated traffic flow</u> and

to a low priority quality of service <u>if it is not associated with a validated traffic flow</u> and placement of data in a quality of service queue based on real time or latency characterization of the data. For example, the subject application recites the following:

> QoS processor 116 takes the conclusion of either or both of header processor 104 and payload analyzer 110 and assigns the data packet to one of its internal quality of service queues 132 based on the conclusion. The quality of service queues 132 can be assigned priority relative to one another or can be assigned a maximum or minimum percentage of the traffic flow through the device. *This allows QoS processor to assign the necessary bandwidth to traffic flows such as VoIP, video and other flows with high quality and reliability requirements while assigning remaining bandwidth to traffic flows with low quality requirements such as email and general web surfing to low priority queues.* Information in queues that do not have the available bandwidth to transmit al the data currently residing in the queue according to the QoS engine is selectively discarded thereby removing that data from the traffic flow.
>
> The quality of service queues 132 **also allow** network apparatus 100 to manage *network attacks such as denial of service (DoS) attacks.* Network apparatus 100 can at to qualify traffic flows by scanning the contents of the packets and *verifying that the contents contain valid network traffic between known sources and destinations.* The traffic flows *that have not been verified* because they are from unknown sources or because they are new unclassified flows can be *assigned to a low quality of service queue until the sources are verified or the traffic flow classified as valid traffic.* Since most DoS attacks send either new session information, data from spoofed sources, or meaningless data, network apparatus 100 would assign those traffic flows to low quality traffic queues.

Subject Application, Page 11, Lines 5-29 (***emphasis added***).

Thus, the subject application is explicit that placement of a data packet in a higher or lower quality of service based on validation/non validation of the traffic is a function performed *in addition* to, and thus distinguished from, placement of data in a service queue based on *high quality and reliability requirements.*

Quite simply, "valid" and "real time" characteristics of a traffic flow are wholly unrelated. Nothing in the subject application, the cited references, or dictionary definitions of the terms indicates any relation between the terms. Moreover, the subject application clearly distinguishes the functions of quality of service placement based on reliability and bandwidth requirements of traffic, and the placement of traffic in a quality of service based on whether the traffic is validated or not.

For the reasons discussed above, Kloth and Lorrain are insufficient to provide a *prima facie* case of obviousness with regard to the claim 1 limitations.

Independent claim 12 recites similar features as claim 1 and was rejected for similar rationale as claim 1. Therefore, the same distinctions between Kloth and Lorrain and the claimed invention in claim 1 apply for claim 12. For the reasons described above, Kloth and Lorrain does not render claim 12 *prima facie* obvious.

Claims 2, 3, and 6 depend from, and further limit, claim 1, and claims 13 and 15 depend from, and further limit, claim 12. Therefore, the same distinctions between Kloth and Lorrain and the claimed invention in claims 1 and 12 apply for claims 2, 3, 6, 13, and 15. For at least this reason, Kloth and Lorrain do not render claims 2, 3, 6, 13, and 15 *prima facie* obvious.

Claims 7, 9, 10, and 11

Claim 7 recites the following:

> 7.   A method of preventing denial of service attacks on a data network which includes a plurality of traffic flows each formed by multiple data packets having header and payload information, the method using a network device comprising a traffic flow scanning engine and a quality of service processor having a low priority queue and higher priority queues, the method comprising:
> scanning the header information using the traffic flow scanning engine;
> reordering and reassembling the data packets using the traffic flow scanning engine;
> flagging data packets that do not reorder or reassemble correctly to be dropped;
> scanning the payload contents using the traffic flow scanning engine;
> determining whether the data packets conform to a set of predetermined requirements;
> flagging data packets that do not conform to be dropped;
> checking if the data packets are associated with a validated traffic flow; and
> assigning data packets to a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if the data packet is not associated with a validated traffic flow.

The Examiner concedes that Kloth does not teach or suggest the claim 7 limitations of "flagging data packets that do not reorder or reassemble correctly to be dropped," "flagging data packets that do not conform" to the set of predetermined requirements "to be dropped," or "assigning data packets to a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if the data packet is not associated with a validated traffic flow." (See Office Action dated 3/10/2005, pages 4-5).

With regard to the steps of "flagging data packets that do not reorder or reassemble correctly to be dropped" and "flagging data packets that do not conform" to the set of predetermined requirements "to be dropped," the Examiner alleges Lorrain discloses such method steps and cites Column 2, Lines 17-19 of Lorrain in support of the rejection of claim 7. Applicants respectfully disagree. For example, Lorrain recites the following:

> In operation, the network traffic must be controlled dynamically requiring that some packets be dropped within the network to avoid traffic jamming. These packets are flagged as discardable packets through use of a so-called Discardable Eligibility (DE) identifier bit.

Lorrain, Column 2, Lines 15-19

Thus, Lorrain only describes flagging packets to be discarded in order to avoid traffic jamming. The packet discarding method described by Lorrain in no manner describes or suggests "flagging data packets *that do not reorder or reassemble correctly* to be dropped" and, for at least this reason, is insufficient in combination with Kloth to render claim 7 prima facie obvious.

Additionally, the method for flagging discardable packets to avoid traffic jamming neither describes or suggests "flagging data packets that do not conform" to the set of predetermined requirements "to be dropped." For at least this reason, Lorrain and Kloth are insufficient to render claim 7 prima facie obvious.

Additionally, as discussed above with regard to the rejection of claim 1, Lorrain clearly fails to describe or suggest a method of "assigning data packets to a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if the data packet is not associated with a validated traffic flow." Rather, Lorrain only describes assignment of a quality of service based on real time or non real time characteristics of traffic. For at least this reason, Lorrain and Kloth are insufficient to render claim 7 prima facie obvious.

Claims 9, 10, and 11 depend from, and further limit, claim 7. Therefore, the same distinctions between Kloth and Lorrain and the claimed invention in claim 7 apply for claims 9, 10, and 11. For at least this reason, Kloth and Lorrain do not render claims 9, 10, and 11 *prima facie* obvious.

Claim 4

-12-

Claim 4 recites the following:

> 4.   The method of Claim 3 wherein scanning includes scanning of the data packet's header information and scanning the data packet's payload contents.

The Examiner alleges that Kloth discloses the method step of "scanning of the data packet's header information and scanning the data packet's payload contents." Applicants respectfully disagree.   The passage of Kloth cited as allegedly disclosing the subject claim limitations is as follows:

> Subsequent packets of detected IP flow are shown as 512, which include an ATM header 514, a payload 516, and IP packet data 518.

Kloth, Column 8, Lines 40-42.

Thus, Kloth only indicates that a flow includes both header and payload data. No description or suggestion is provided for "scanning of the data packet's header information and scanning the data packet's payload contents" as described in the subject application and explicitly recited in the subject claim. For at least this reason, Lorrain and Kloth are insufficient to render claim 4 prima facie obvious.

Claims 5, 8, and 16

Claim 5 recites the following:

> 5.   The method of Claim 1 wherein the predetermined requirements include packet length, non-overlapping offset fields, and adherence to protocol standards,

The Examiner alleges that Kloth discloses a method of verifying that data packets conform to a set of predetermined requirements including "packet length, non-overlapping offset fields, and adherence to protocol standards." Applicants respectfully disagree. The passage of Kloth cited as allegedly disclosing the subject claim limitations is as follows:

> Accordingly, the present system performs the route lookup in parallel to the lookup of the rest of the attributes of the particular packet, i.e. both lookups are done in parallel.

Lorrain, Column 4, Lines 5-8

Thus, the passage of Kloth only describes a look up of packet "attributes." Kloth in no manner describes, suggests, or otherwise alludes to a method of verifying that data packets conform to a set of predetermined requirements including "packet length, non-overlapping offset

fields, and adherence to protocol standards" as described in the subject application and explicitly recited in the subject claim. For at least this reason, Lorrain and Kloth are insufficient to render claim 5 prima facie obvious.

Claims 8 and 16 recite similar subject matter as claim 5 and were rejected for the same rationale as claim 5. Therefore, the same distinctions between Kloth and Lorrain and the claimed invention in claim 5 apply for these claims. For at least this reason, Lorrain and Kloth are insufficient to render claims 8 and 16 prima facie obvious.

Moreover, claims 5, 8, and 16 respectively depend from and further limit claims 1, 7, and 12 already demonstrated to be in condition for allowance. Therefore, claims 5, 8 and 16 are also allowable, at least by virtue of their dependence on an allowable base claim.

Claim 14

Claim 14 recites the following:

> 14. The network device of Claim 12 wherein data packets that do not reorder or reassemble correctly and data packets that do not conform to the predetermined requirements are dropped by the network device.

The Examiner alleges that Kloth discloses a method of dropping data packets that "do not reorder or reassemble correctly and data packets that do not conform to the predetermined requirements." Applicants respectfully disagree. The passage of Kloth cited as allegedly disclosing the subject claim limitations is as follows:

> There might still be a portion of data packets that are in transition, and might cause the transmitting station to re-send the packet. Therefore, it is better to cut off such packets altogether. Decision block 1010 inquires whether the system load is within an acceptable range. If not, the step 1012 directs the system to discard packets for certain service levels.
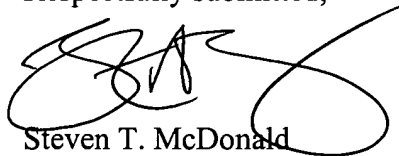
Kloth, Column 12, Lines 5-10.

Thus, Kloth only describes dropping packets of certain service levels if the system load is not within an acceptable range. Kloth in no manner describes, suggests, or otherwise alludes to dropping data packets that "do not reorder or reassemble correctly and data packets that do not conform to the predetermined requirements." For at least this reason, Lorrain and Kloth are insufficient to render claim 14 prima facie obvious.

II. Conclusion

Accordingly, it is respectfully submitted that the references alone or in combination do not disclose or suggest the subject matter of claims 1-16.

For all of the foregoing reasons, it is respectfully submitted that claims 1-16 be allowed. A prompt notice to that effect is respectfully requested.

Respectfully submitted,

Steven T. McDonald
Registration No. 45,999

Dated: 10 August 2005

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 972/739-8644
Facsimile: 972/692-9075
R112898

CLAIMS APPENDIX

1. A method for preventing denial of service attacks over a data network including a plurality of traffic flows each formed by a plurality of data packets, the method comprising:

scanning the contents of the data packets;

verifying that the data packets conform to a set of predetermined requirements;

checking if the data packet is associated with a validated traffic flow; and

placing the data packet in a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if it is not associated with a validated traffic flow.

2. The method of Claim 1 wherein verifying includes insuring that the data packets reorder and reassemble according to a defined policy and insuring that the data packets conform to required parameters.

3. The method of Claim 1 further comprising between verifying and checking:

dropping the data packet if it does not conform to the set of predetermined requirements.

4. The method of Claim 3 wherein scanning includes scanning of the data packet's header information and scanning the data packet's payload contents.

5. The method of Claim 1 wherein the predetermined requirements include packet length, non-overlapping offset fields, and adherence to protocol standards.

6. The method of Claim 5 wherein the validated traffic flows are identified by a state associated with each traffic flow.

7. A method of preventing denial of service attacks on a data network which includes a plurality of traffic flows each formed by multiple data packets having header and payload information, the method using a network device comprising a traffic flow scanning engine and a quality of service processor having a low priority queue and higher priority queues, the method comprising:

scanning the header information using the traffic flow scanning engine;

reordering and reassembling the data packets using the traffic flow scanning engine;

flagging data packets that do not reorder or reassemble correctly to be dropped;

scanning the payload contents using the traffic flow scanning engine;

determining whether the data packets conform to a set of predetermined requirements;

flagging data packets that do not conform to be dropped;

checking if the data packets are associated with a validated traffic flow; and

assigning data packets to a higher priority quality of service if the data packet is associated with a validated traffic flow and to a low priority quality of service if the data packet is not associated with a validated traffic flow.

8. The network device of Claim 7 wherein the set of predetermined requirements include packet length, non-overlapping offset fields, and adherence to protocol standards.

9. The method of Claim 7 wherein flagged data packets are dropped by the traffic flow scanning engine.

10. The method of Claim 7 wherein flagged data packets are dropped by the quality of service processor.

11. The method of Claim 7 wherein the validated traffic flows are identified by a state associated with each traffic flow.

12. A network device for preventing denial of service attacks on a data network which includes a plurality of traffic flows each formed by multiple data packets having contents including header information and payload information, the network device comprising:

a traffic flow scanning engine operable to scan the header and payload information of the data packets, to associate each data packet with a particular traffic flow and to determine whether each traffic flow is a validated traffic flow or a non-validated traffic flow, wherein the traffic flow scanning engine is further operable to reorder and reassemble the data packets and to verify

that the data packet conforms to predetermined requirements such that the traffic flow scanning engine produces a conclusion associated with each data packet; and

a quality of service processor connected to the traffic flow scanning engine and operable to place the data packets into a quality of service queue from a plurality of quality of service queues based on the conclusion from the traffic flow scanning engine, wherein data packets from non-validated traffic flows are assigned to a low priority queue and data packets from validated traffic flow are assigned to a higher priority queue based on its contents.

13. The network device of Claim 12 wherein the low priority queue is assigned a maximum percentage of network bandwidth.

14. The network device of Claim 12 wherein data packets that do not reorder or reassemble correctly and data packets that do not conform to the predetermined requirements are dropped by the network device.

15. The network apparatus of Claim 12 wherein the traffic flows are identified by a state associated with each traffic flow, the state representing whether the traffic flow is validated or non-validated.

16. The network apparatus of Claim 12 wherein the set of predetermined requirements include packet length, non-overlapping offset fields, and adherence to protocol standards.